UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,288	03/06/2002	Pekka Nikander	3772-8	5575

23117 7590 07/22/2005

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PRIETO, BEATRIZ	

ART UNIT	PAPER NUMBER
2142	

DATE MAILED: 07/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/091,288	NIKANDER, PEKKA	
	Examiner	Art Unit	
	Prieto B.	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) *12-16,21 and 22* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 17-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 March 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *03/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to Election Restriction Requirement Response mailed 07/06/05, election of the invention of Group I (claims 1-11 and 17-20) for further substantive examination is acknowledge. Claims 12-18 and 21-22 are thereby withdrawn from consideration.

Drawings

2. Drawings have been objected to by examiner. In this case on Figure 1, there is an network entity component missing reference number, Internet network (5) and what seems to be a computer (5) have the same reference number. Applicant is urged to further review the drawings. A proposed drawing correction or corrected drawings are required in reply to this office action to avoid abandonment of the application. The objections to the drawings are no longer held in abeyance. If reply does not include corrected drawings, proposed corrections, or reply to the drawings requirement, the reply would be held non-responsive (See MPEP §1.85 revised, 65 FR 54604, Sept. 8, 2000, effective Nov. 7, 2000; para. (a) revised, 65 FR 57024, Sept. 20, 2000, effective Nov. 29, 2000).

Claim Objection

3. The following claims are objected to because of the noted following informalities, claim 7 recites, said series sequence of hash values, this clause lacks antecedent basis. Claim 17, 'carrying out the method of the above first aspect of the of the invention to confirm that said host is authorized to use the IP address", it is respectfully noted that: (i) it is not clear what "above first aspect" this clause refers to or seems to lack antecedent basis, and (ii) to "confirm that said host is authorized to use the IP", seems to be an intended purpose or objective that does provide limiting structure or further limits the scope in structurally (see MPEP §2111.02).

Claim Rejection under 35 USC 103

4. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman, et. al. U.S. 5,351,295 (referred to as Perlman hereafter) in view of Ford et. al. (US 6,101,499) (referred to as Ford hereafter).

Regarding claim 1, Perlman teaches a method comprising a stations or nodes ("host") coupled to a communication "IP" network (col 1/lines 15-23), the host using an address (col 2/lines 6-8), the method comprising:

applying a one-way coding function to a value "component" sent from the host, e.g. sender's address by a receiving station for authenticating the received value (col 2/lines 63-66, col 4/lines 42-51), and

if the result matches the interface identifier the host is assumed to be authentic, authorized to use the address, where a legitimate host is using its address, the and if the result does not match the interface identifier the host is assumed not to be authorized to use the address, where an legitimate station has been impersonated by using its address, and the receiving host takes the appropriate response when a match is found (col 2/lines 49-col 3/line 2, figs. 1-3, steps 18, 30, 36);

however Perlman teaches the use on the sender's address contained in the data link header (i.e. a portion of an address), she does not explicitly teach where the host uses an "IP" address, the address comprising a first portion/part "routing prefix" and a second portion "interface identifier".

Ford teaches the use by hosts of an address (called IP), the address comprising a first portion/part (called routing prefix) and a second portion (called interface identifier) (col 2/lines 12-27), where applying a one-way coding function to a value of the host, such as an interface identifier (col 9/lines 4-9) generate at value used as an address.

It would have been obvious to one ordinary skilled in the art at the time the invention was made given the teaches for verifying that a host is authorized to use an address, where an eavesdropper is not impersonating a legitimate host by using its address and suggestions for using an identifier which is unique to the host the teachings of Ford for automatically generating a unique identifier would have been readily apparent. One would be motivated to utilize an IP address of any format or any portion thereof automatically generated and ensuring that a legitimate host is using a provided IP address.

5. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman, et. al. U.S. 5,351,295 (referred to as Perlman hereafter) in view of Internet Draft: Privacy extensions for stateless address auto-configuration in IPv6, Thomas Narten, IBM, June 1999 (referred to as Narten hereafter).

Regarding claim 1, Perlman teaches a method comprising a stations or nodes ("host") coupled to a communication network (called IP) (col 1/lines 15-23), the host using an address (col 2/lines 6-8), the method comprising:

applying a one-way coding function to a value (called component) sent from the host, e.g. sender's address by a receiving station for authenticating the received value (col 2/lines 63-66, col 4/lines 42-51), and

if the result matches the interface identifier the host is assumed to be authentic, authorized to use the address, where a legitimate host is using its address, the and if the result does not match the interface identifier the host is assumed not to be authorized to use the address, where an legitimate station has been impersonated by using its address, and the receiving host takes the appropriate response when a match is found (col 2/lines 49-col 3/line 2, figs. 1-3, steps 18, 30, 36); however Perlman teaches the use on the sender's address contained in the data link header (i.e. a portion of an address), she does not explicitly teach where the host uses an address (called IP), the address comprising a first portion/part (called routing prefix) and a second portion (called interface identifier).

Narten teaches the use by hosts of an address (called IP), the address comprising a first portion/part (called routing prefix) and a second portion (called interface identifier) (p. 2), where applying a one-way coding function, e.g. MD5 hash to a value of the host, such as an interface identifier (p. 6) generate at value used as an address.

It would have been obvious to one ordinary skilled in the art at the time the invention was made given the teaches for verifying that a host is authorized to use an address, where an eavesdropper is not impersonating a legitimate host by using its address and suggestions for using an identifier which is unique to the host the teachings of Ford for automatically generating a unique identifier would have been readily apparent. One would be motivated to utilize an IP address of any format or any portion thereof automatically generated using history values or randomly generated sequence of hash values and ensuring that a legitimate host is using a provided IP address.

Regarding claim 2, said component comprise a "hash" value being one of a sequence of related values (Perlman, col 2/lines 53-55), hash value being one of a sequence of iterations (Narten: p. 6).

Regarding claim 3, said components comprise a shared secret (i.e. public key) generated by said host or obtained by said host from another authorized party (Perlman: col 2/lines 40-48).

Regarding claim 4-5, said components comprise an "initial interface" identifier corresponding to link layer address of the host (Perlman: col 2/lines 6-8, Narten, initial boot time value p. 6).

Regarding claim 6, said components comprise a counter value to control the iteration sequence in the algorithm (Narten, p. 6), which identifies the next history value to be used ("position") of the received hash value in said sequence iteration (Narten: p. 6).

Regarding claim 7, said series of iteration each generating a sequence of hash values in step (2) of the iteration (Narten, p. 6) are derived at the host by applying a one-way coding function to a random number "seed value" and a shared secret "public" key (Perlman: col 2/lines 63-66, col 4/lines 42-51, Narten, seed value, p. and pseudo-random sequence p. 6).

Regarding claim 8, wherein said series of iterations of hash values are derived at the host by applying a one-way coding function to a seed and an initial interface identifier (Narten, p. 6).

Regarding claim 9, series of iterated hash values are derived at the host by applying a one-way coding function to a seed, an initial interface identifier, as discussed on claim 8, and further a share secret "public" key (Perlman: col 2/lines 63-66, col 4/lines 42-51).

Regarding claim 10, deriving a hash value from the received hash value to provide a value "derivative" to which the one-way coding function is applied, the derived hash value being the last hash value in the iteration based on the previous value iteration (Narten, p. 6).

Regarding claim 11, wherein in the event of a first IP address verification, the hash value received from the host is the hash value preceding the final hash value in the sequence and for each subsequent verification process, the next previous hash value must be received from a stable storage (Narten, p. 6).

Claim Rejection under 35 USC 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 17-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Hellman (US 5,872,917).

Regarding claim 17, Hellman teaches a user host coupled to a network accessing a server computer (col 1/lines 9-35), the host is able to receive data packets sent to that address, i.e. the address of the host where messages are sent to, i.e. using a the host address as a destination address, wherein, e.g. a dial-up telephone connection over the Internet uses an IP based addressing scheme (col 2/lines 13-36, col 1/lines 18-35), the method comprising:

sending a message "challenge" to the host (col 2/lines 37-49, col 3/lines 41-49);

receiving a response from the host (col 2/lines 37-49, col 3/lines 41-49); and

verifying that the received response is a correct response to the challenge (col 2/lines 37-49, col 3/lines 41-49 and col 6/lines 36-56).

Regarding claim 18, said challenge comprises a randomly generated number (Hellman: col 2/lines 37-42, col 6/lines 57-67) and the response comprises the challenge (Hellman: col 2/lines 42-45

8. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable Hellman in view of Internet Draft: Privacy extensions for stateless address auto-configuration in IPV6, Thomas Narten, IBM, June 1999 (referred to as Narten hereafter).

Regarding claims 19-20, however Hellman teaches randomly generated number to which a one-way function is applied, he does not teach concatenating an address with a randomly generated number

Narten teaches appending "concatenating" an IP address portion with a 64-bit value, predetermined or randomly generated (Narten: p. 6) and applying a one-way coding function to this combination (Narten p. 6)

It would have been obvious to one ordinary skilled in the art at the time the invention was made given the teachings of Hellman for authenticating a user, the teachings of Narten for authenticating a user by detecting un-legitimate users using others IP addresses would be readily apparent. One would be motivated to One would be motivated to utilize an IP address of any format or any portion thereof automatically generated using history values or randomly generated sequence of hash values and ensuring that a legitimate host is using a provided IP address.

Citation of Pertinent Art

9. The following prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Copies of Non-Patent Literature documents cited will be provided as set forth in MPEP§ 707.05(a):

US 6,904,456

Cox teaches an IP address comprising a routing prefix and an interface identifier part, a host coupled to a network, using said IP address.

US 6,542,508

Lin teaches policy binding database to associate data packet, the method computes applying a one-way function to a data packet, including a hash value (or use some other identification function) from the well known fields (which uniquely identify a stream) of the packet to find its corresponding policy decisions (action specifications 210), wherein specific value may include an IP addresses or any user specifiable criteria.

US 5,958,053

Denker applying for security reasons a one-way coding function to generate a component/encoded value, calculated by a receiving host server as a crypto logic function (or other mathematical function) that depends upon at least the IP address of client and a secret key value. The encoded value can be a crypto logic function which depends upon one or more additional parameters (in addition to the secret and the IP address), including an IP address and a sequence number; the encoded value can be calculated by server as follows obtaining the encoded value calculated as the one-way function (e.g. MD5 hash) of the IP address and the random secret value plus and initial sequence number.

US 5,845,267

Ronen teaches sending a message to a host using the IP address of the host as the address destination of the message. Specifically, as well known routers routes packets through Intranet to and from destinations on the Intranet or Internet in accordance with the destination address in each packet, where the IP address assigned to user terminals are further bind to the user identity.

US 4,701,745

Waterworth an input store for receiving and storing a plurality of bytes of data from an outside source, means for processing successive bytes of data from the input store, the data processing means including circuit means operable to check whether a sequence of successive bytes already processed, and including hash generating means responsive to the application of a predetermined number of bytes in sequence to derive a hash code appropriate to these bytes, a temporary store in which the hash code may represent the address of a storage location, and a pointer counter operable to store in the temporary store at said address a pointer indicative of the position in the input store of one of the predetermined number of bytes.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Prieto, B. whose telephone number is (571) 272-3902. The Examiner can normally be reached on Monday-Friday from 6:00 to 3:30 p.m. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's Supervisor, Andrew T. Caldwell can be reached at (571) 272-3868. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3800/4700.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system, status information for published application may be obtained from either Private or Public PAIR, for unpublished application Private PAIR only (see http://pair-direct.uspto.gov or the Electronic Business Center at 866-217-9197 (toll-free).

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Hand carried or delivered to:
Customer Service Window located at the Randolph Bldg.
401 Dulany St.
Alexandria, VA 22314

Faxed to the Central Fax Office:
(703) 872-9306 (old No. in service until Sept. 15, 2005),
(571) 273-8300 (New Central Fax No.)

Or Telephone:

(703) 306-5631 for TC 2100 Customer Service Office.

Beatriz Prieto

BEATRIZ PRIETO
PRIMARY EXAMINER

B. Prieto
TC 2100
Primary Examiner
July 21, 2005